# Should You Password Protect Your Cell Phone?

*by*

Phil Rasmussen

In today's digital age, cell phones have become an integral part of our daily lives. We use them to communicate, browse the internet, access social media, and store personal and financial information. The convenience of cell phone usage also has a lot of risks.

With cybercriminals becoming increasingly sophisticated there is a lot of debate on whether you should password protect or encrypt your cell phone. While the debates persist, technology will continue evolving, other operating systems will emerge for cell phones, and that there are specific reasons why selected cell phones need to be encrypted.

As mentioned there are some compelling reasons why some cell phones need to be encrypted. These reasons generally apply to cell phones used for business. Before we go further, let's understand that business cell phones should be restricted to business use only. Conversely personal cell phones also have their restrictions.

Here are three reasons why business cell phones need to be encrypted.

- Ensures compliance with regulations and standards related to data protection, avoiding legal liability, financial loss, and reputational damage.
- Safeguards sensitive business data, such as confidential documents, financial records, and proprietary information.
- Provides an additional security measure to protect against data breaches and unauthorized access to business information.

But what about personal cell phones, should they be encrypted? There is not a straight answer to this question. To begin with we need to answer the question, "What is the purpose for you to buy a cell phone?" The answer is typically, "So that I can call family, friends, etc." If that is your answer then ask yourself, "Why did you buy a smartphone?" Now this is where the waters get muddied.

The differences between cell phones and smartphones are:

- Cell phones are used only for telephone calls and many have built-in address books.
- Smartphones are like miniaturized computers. While they are generally used for telephone calls, they also have applications, which are built into them or can be added.

Most people buy smartphones when they sign up for cell phone and/or Internet service. Although they may be thinking of using their smartphone initially for phone calls, the temptation to explore and use other applications on these phones is hard to resist. Just like many temptations, once tried, you're hooked.

Among the first things that most apps require are access to such areas as your location, email address, address book, passwords, and other built-in applications on your smartphone. Many apps that you install also access other information through "backdoor" processes.

The development of quantum computing and AI has opened up the entire Internet and all email systems to hacking. Secure email gateways (SEGs), security software used to encrypt emails, are no longer secure. Regardless of the email system you use, sophisticated hackers can access your computers and smartphones with ease.

Although hackers can access your phone with ease, this does not mean you should not consider protecting it. The most common form is to simply install a password. Other approaches include one or more encryption processes.

| | |
|---|---|
| **Data Protection** | Encryption protects your personal data, such as text messages, emails, photos, and financial information, from unauthorized access or theft. |
| **Privacy Preservation** | With encryption, your online activities and communications remain private, shielding you from surveillance and data breaches. |
| **Compliance** | Many industries have strict data privacy regulations, and encryption helps ensure compliance with these standards. |
| **Remote Data Wiping** | Some encrypted devices allow remote data wiping, enabling you to securely erase all data from a lost or stolen device. |
| **Full Disk Encryption (FDE)** | FDE encrypts all data, applications, and the operating system. This ensures that no data can be accessed without the proper decryption key. |
| **File/Folder Encryption** | You can selectively encrypt specific files or folders on your phone as desired |
| **Communication Encryption** | Messaging apps use end-to-end encryption to secure your conversations, preventing others from intercepting and reading your communications. |

The choice is yours. You can password protect your phone and/or use different forms of encryption. A better approach however would be to resist downloading and installing apps which make it easier to hack your phone, and using your phone for making phone calls. If you need applications, select ones that do not collect or require access to your

personal information.  Those apps, and the data created while using them, can be encrypted.

As mentioned, it is easier for most of us to simply password protect our phones. However, this is not a good idea.

When an emergency occurs, your adrenaline spikes, fine motor skills greatly diminish, and confusion sets in.  Trying to remember one of many passwords that you use becomes harder and inputting it into a phone becomes more time consuming, especially since most passwords are not 6 or more characters.  It is far easier to hit the call button on the phone and dial 911.

Similarly if you are in an accident and your phone is password protected, others cannot easily call for assistance and responders will not be able to get vital information, such as medical or next-to-kin information.  This inability to access your phone can dramatically increase your health and other risks.  Your phone directory should always have an "In Case of Emergency" or ICE or SOS listing.

You can set your emergency contact information on most smartphones by going to the settings menu for the phone.  Additionally you should also create either an ICE or SOS contact in your phone directory for your emergency contact information.  The information should include

- Name of person to contact
- Relationship to the person
- Their phone number and email address
- Any medical conditions you have

For android phones, follow the instructions on the Mad Penguin website at:

https://www.madpenguin.org/how-to-set-emergency-contact-on-android/

iPhones users have two methods for setting up emergency contact information.  Be sure to read the instructions on both Tech Edvocate and GB Times websites and do both setups.

- https://www.thetechedvocate.org/how-to-set-up-emergency-contacts-on-iphone/
- https://gbtimes.com/how-to-make-emergency-contacts-on-iphone/

**Set your emergency Contact information now!**